An Analysis of Information Leakage from a Cryptographic Hardware via Common-Mode Current

Yu-ichi Hayashi#1, Takeshi Sugawara#2, Yoshiki Kayano†1, Naofumi Homma#
Takaaki Mizuki#, Akashi Satoh*1, Takafumi Aoki#, Shigeki Minegishi‡1, Hideaki Sone#, Hiroshi Inoue†
Tohoku University
1 yu-ichi@mail.tains.tohoku.ac.jp ,2sugawara@aoki.ecei.tohoku.ac.jp
†Akita University
1kayano@venus.ee.akita-u.ac.jp
* National Institute of Advanced Industrial Science and Technology
1Akashi.satoh@aist.go.jp
‡Tohoku Gakuin University
1smine@tjcc.tohoku-gakuin.ac.jp

***Abstract*— This paper analyzes the propagation of information leaked from cryptographic modules via common-mode current. We propose a simple board model in order to discuss the leakage mechanism in a general manner. Our simulation and experimental results show that the frequency characteristic of the proposed board model agrees rather well with those of a real cryptographic board. Based on these results, we propose that there needs to be a discussion on security countermeasures from the view of both EMC and side channel attack.**

Key words: side-channel attack, electromagnetic security, common-mode current

I. INTRODUCTION

It is known that cryptanalysis based on side-channel information, such as transient current and near-field radiation, released from cryptographic modules can reveal the secret information stored in the modules. Such attacks are called side-channel attacks and of major concern for designers of smartcards and other embedded cryptosystems. Fig. 1 shows an example of transient current captured from a hardware implementation of the ISO/IEC standard block cipher Advanced Encryption Standard (AES) [1]. The AES circuit is designed to operate the encryption process with 11 rounds. The waveform in Fig. 1 clearly shows 11 peaks corresponding to the encryption rounds. Side-channel attacks extract secret information from such waveforms correlated to the intermediate data being processed.

Previous studies on side channel attacks have focused mainly on how to extract secret keys from measured waveforms of current, voltage or electromagnetic field, assuming that the waveforms include significant information available for the attacks. In other words, they did not fully discuss where the information can be measured.

This paper analyzes where/why we can obtain such waveforms from the EMC point of view. We first propose a general module model to analyze the propagation of information via common-mode current, and then show that the simulation result is closely related to an experimental result with an actual cryptographic hardware. Based on these results, we discuss how an effective countermeasure against side-channel attacks can be applied.

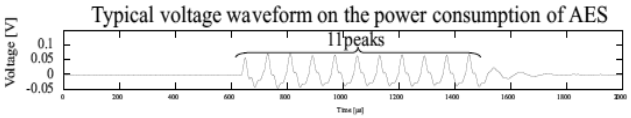

Fig. 1 A typical Power Waveform of AES

II. SIDE CHANNEL FROM THE EMC POINT OF VIEW

A power-analysis attack, which is one of the most powerful side-channel attacks, utilizes a number of transient currents measured from a target cryptographic hardware. The total current of a CMOS circuit essentially depends on the number of logic cells processed by the input signal, and the current waveforms measured by a digital measurement device (e.g., a digital oscilloscope) often include the dependency. For example, Differential Power Analysis (DPA) [2] performs a statistical analysis of the waveforms in time domain to reduce the noise and retrieve the secret information. The waveforms have been measured at module's power/GND plane.

However, we assume that there is a definite possibility of measuring secret information at further

points if the above transient current is available for the attacks. The assumption is based on the fact that the transient current causes ground bounce which generates common-mode current [3][4] being distributed on the board and the attached cables. Thus, we focus on common-mode current to explain the mechanism of the information leakage.

The cryptographic module considered here is composed of many circuit elements including active ones. In order to discuss the leakage mechanism in a general manner, we propose a simple board model which is sufficient to describe the characteristics of the cryptographic modules related to power analysis. An overview of the proposed model is showen in Fig. 2. Based on the proposed model, we discuss how the transient current is conducted to various parts of the board in the form of common-mode current. Indeed, the authors conducted a measurement on a cable attached to Side channel Attack Standard Evaluation Board (SASEBO) [5]. In the measured waveform, a specific shape similar to Fig. 1 is observed. The result suggests that the transient current is conducted to the cable as predicted. From security point of view, this result indicates that an adversary could attack a security system by measuring it from a distance.

III. Experimental and Modeling Methods

In this section, we present a measurement setup and the corresponding simulation method to measure and compute the common-mode current caused by transient current on the proposed board model.

A. *Measurement Setup*

Common-mode current on the proposed board with a cable was measured using a current probe (Fischer F-2000) and a spectrum analyzer with tracking generator (Advantest R3131A), as shown in Fig. 23. A 1000 mm × 1000 mm aluminum plate was used to isolate the measured system (i.e., the board with the cable) from the measurement system (i.e., the spectrum analyzer). The tracking generator was connected to the board via a semi-rigid cable ("Drive Point" in Fig. 2), and voltage was driven 120dBμV to simulate the transient current (Fig. 3). The current probe was fixed at 75mm from the aluminum plate and was connected to the input port of the spectrum analyzer. Here we fixed the probe near the aluminum plate in order to prevent the measurement from being influenced by electric coupling occurred between the probe and the power line or the board with the cable.

The length and width of the board (PCB_l and PCB_w) were 250 and 200 mm, respectively. The length of the power line (PL_l) was 250 mm, and the length of the semi-rigid cable ($Semi_l$) was 150 mm.

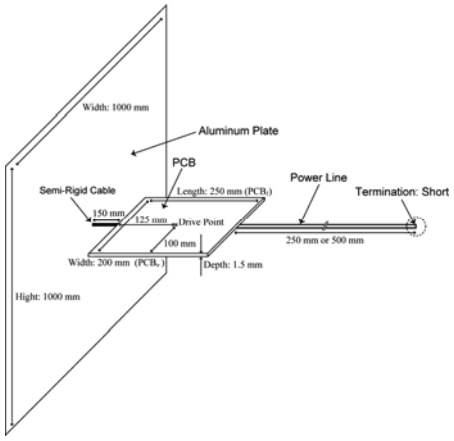

Fig. 2 Measurement System of Common-mode Current Using a Model Board

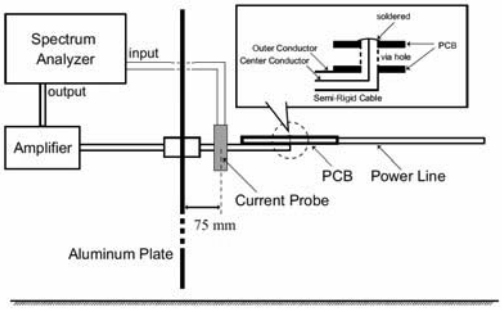

Fig. 3 Driving voltage to the Model Board

B. *FDTD Simulation for Board with Cable*

The finite difference time domain (FDTD) method is used for the field simulation and calculation of the Common-mode current on the board with cable. The cell size of the simulation was as follows: dx = dy = 5 mm, dz = 0.765 mm. From Courant stability condition we set dt = 2.49 ps. The board with cable was modeled as a perfect conductor. The aluminum plate was also modeled as a perfect conductor, and as an infinite ground plane.

Relative permittivity of the dielectric in the board was ε_r = 4.5. The source was modeled as a voltage source with an internal resistance of 50 Ω to take account of the 50 Ω measurement systems. A sinusoidally modulated Gaussian pulse voltage was applied as the signal waveform. The common-mode current was calculated from loop integral of the magnetic field around the cable at the probe position.

IV. Measurement of Common-mode Current on the Proposed Board

Results of the actual measurement and simulation are shown in Fig. 4 (top: the frequency characteristic of common-mode current, bottom: reflection coefficient). In Fig. 4, we can consider two parts of frequency bands: Bands (1) and (2). The peak

frequency band which changes depending on the length of the cable attached to the board appears in Band (1), and the peak frequency band which does not depend on the length is shown as Band (2).

A. *Frequency Band depending on Cable Length*

In this section, we focus on Band (1). It is assumed that resonance in this band is caused by both pattern of the board and the length of cable [6][7][8]. Since the total length (Total$_l$) of the measured system was 850 mm, the resonance was occurred on 91 MHz (i.e., the wavelength λ_{91} = 3.3 m) in Band (1) by the FDTD simulation. the wavelength $\lambda_{91}/4$ is 824 mm and is nearly equal to Total$_l$. Thus the simulation result was in excellent agreement with the resonance in this band caused by the both pattern of the board and the length of the cable.

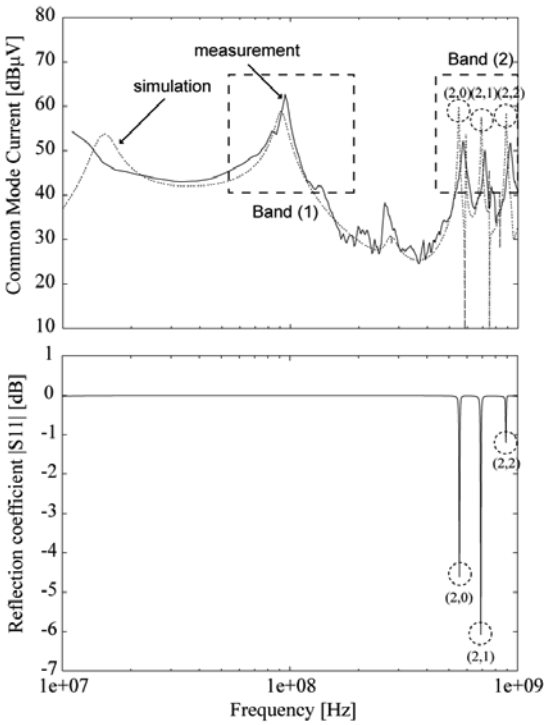

Fig. 4 Frequency Characteristics of Common-mode Current

B. *Frequency Band not Depending on Cable Length*

Band (2) of Fig. 4 is cavity resonance of the board [8][9].

Cavity resonance frequency is expressed as Eq. (1) (m = 0, 1, 2 … n = 0, 1, 2 …), where ε_r = 4.5, PCB$_w$ = 200 mm, PCB$_l$ = 250 mm:

$$f_r = \frac{150}{\sqrt{\varepsilon_r}} \sqrt{\left(\frac{m}{PCB_w}\right)^2 + \left(\frac{n}{PCB_l}\right)^2} \qquad (1)$$

Tab. 1 shows the resonance frequencies in cases when (m, n) are (0,0) to (3,3).

Tab. 1 Cavity Resonance Frequencies

		m			
		0	1	2	3
n	0		283	**566**	849
	1	353	452	**667**	919
	2	707	761	**905**	1104
	3	1061	1098	1202	1358

The bottom of Fig. 4 shows the reflection coefficient S11 at the input port of the board. The peaks of Band (2) in the upper of Fig. 4 agree with those in the bottom figure, which shows the resonance frequencies when (m, n) = (2, 0), (2, 1), (2, 2) shown in Tab. 1. Thus, the resonances in this band are based on the cavity resonance on the board.

V. Common-mode Current on Cryptographic Hardware

This section shows an experiment using SASEBO, where an AES algorithm is implemented with an FPGA. We measured common-mode current on a semi-rigid cable by inputting sinusoidal waves of 1 MHz to 1 GHz at 120dBμV.

The results are shown in Fig. 5. Frequency characteristic of the common-mode current is also classified into two bands: one is dependent on the length of cable attached to SASEBO and another is independent on it. Fig. 6 shows the frequency characteristic of transient current in SASEBO (i.e., the frequency characteristic of Fig.1). Actually leaked common-mode current is given as a product of the two frequency characteristics in Fig. 5 and Fig. 6.

The results of Fig. 4 and Fig. 5 show that the frequency characteristic of the proposed (simple) board model agrees rather well with those of a real cryptographic board measured on the attached cable via common-mode current, even if the cryptographic board was implemented with many circuit elements.

Fig. 7 shows a measured common-mode current on the power line (3m) attached to SASEBO using the current probe at 0.45m from the board, where the AES algorithm is performed. We can observe that there appear 11 peaks in Fig. 7 similarly to Fig. 1.The result indicates that the transient current appearing in a cryptographic module keeps its characteristic waveform though the current changes to common-mode current. Thus we can say that the waveform is measurable wherever the common-mode current can be propagated on the board and the attached cable.

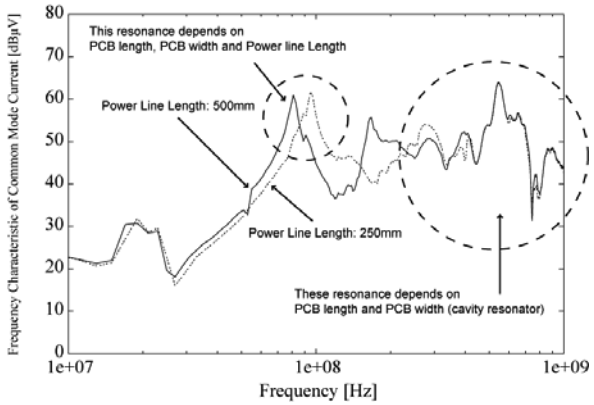

Fig. 5 Common-mode Current generated on Cryptographic Hardware.

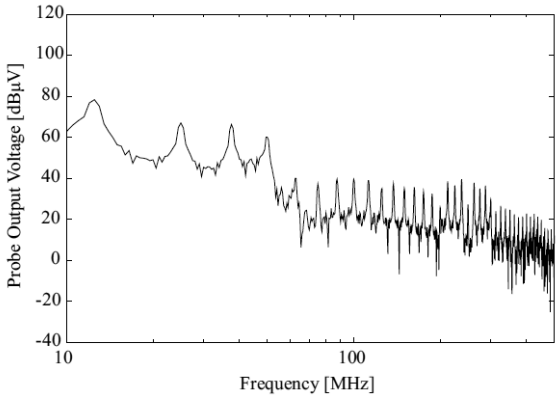

Fig. 6 Frequency Characteristics of Transient Current on Cryptographic Hardware

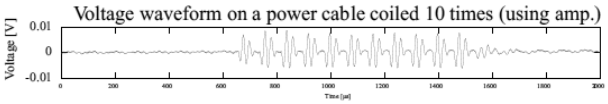

Fig. 7 Voltage on Power Line (twisted) Attached to SASEBO

VI. DISCUSSION

As mentioned above, we showed that the waveforms of characteristic shapes can be obtained around the attached cable. This means that the waveforms are determined by the common-mode current. The waveform shape correlated with the typical power waveform implies that they include the secret key information available for power-analysis attacks. Thus, the secret key information may probably leak via near-field radiation.

We observe from the results in Section V that the secret key information is included on a particular frequency and it matches the resonance frequency of Antenna. The observation suggests that a factor of EMI model can enhance the propagation of the secret key information leaks. Therefore, we need to devise countermeasures with caring about the radiation characteristic of device including attached cables.

VII. CONCLUSION

This paper analyzed where/why we can obtain waveforms including secret information from the EMC point of view. Our analysis shows that secret key information is leaked outside the cryptographic board via common-mode current, where as the information has been considered to be extracted just only near the cryptographic module. We also pointed out the possibility of leakage of private key information around the cryptographic hardware because common-mode current is well known as a main factor of EMI radiation. Furthermore, the mechanism that the secret key is leaked outside of the cryptographic device was shown based on the EMI model by experiment and simulation. To provide secure and safe environment of information communication, we believe that EMC regulations should be innovated for reducing unnecessary radiation when cryptographic module is designed. In addition to the regulations, we also need to discuss a new tamper-resistance capability to prevent the information leakage from the view of both EMC and side channel attack.

Acknowledgments

Computation time was provided by the Super Computer System, Cyberscience Center, Tohoku University.

VIII. REFERENCES

[1] NIST FIPS PUB. 197, Advanced encryption standard (AES), http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

[2] P.C.Kocher, J.Jaffe and B.Jun, "Differential power analysis," Proc. CRYPTO, LNCS, vol.1666, Springer, pp. 388–397, 1999

[3] T.Sudo, H.Sasaki, N.Masuda and J.Drewniak, "Electromagnetic interference (EMI) of system-on-package (SOP)," IEEE Trans. Advanced Packaging, 27(2), pp. 304–314, 2004

[4] Y.Yang and J.Brews, "Design trade-offs for the last stage of an unregulated, long-channel CMOS off-chip driver with simultaneous switching noise and switching time considerations,"IEEE Trans. Advanced Packaging, 19(3), pp. 481–486, 1996

[5] Side-channel Attack Standard Evaluation Board (SASEBO), http://www.rcis.aist.go.jp/special/SASEBO/index-en.html

[6] J.Drewniak, F.Sha, T.Van Doren, T.Hubing, J.Shaw, "Diagnosing and modeling common-mode radiation from printed circuit boards with attached cables," In IEEE International Symposium on Electromagnetic Compatibility, 1995. EMC 1995, pp. 465–470, 1995

[7] D.Hockanson, J.Drewniak, T.Hubing, T.Van Doren, F.Sha and M.Wilhelm, "Investigation of fundamental emi source mechanisms driving common-mode radiation from printed circuit boards with attached cables," IEEE Trans. on Electromagnetic Compatibility 38(4), pp. 557–566, 1996

[8] Y.Kayano, M.Tanaka and H. Inoue, "Identifying the frequency response of common-mode current on a cable attached to a pcb," IEICE transactions on electronics, vol. E87c, no.8, pp. 1268–1276, 2004

[9] T.Fischer, M.Leone and M.Albach, "An analytical model for studying the electromagnetic radiation of power-bus structures," In IEEE International Symposium on Electromagnetic Compatibility, 2003. EMC 2003, vol. 221, pp. 225–230, 2003